MEMORANDUM FOR THE RECORD

FROM: JUDITH SPENCER
CHAIR FEDERAL PKI STEERING COMMITTEE

SUBJECT: Trip Report for APEC TEL 26, August 17-23, 2002, Moscow, Russia

I attended the subject meeting at the request of the U.S. Head of Delegation, Joseph Richardson (US State Department), as a subject matter expert on Public Key Technology within the United States government. My participation was limited to participation in two workshops: the EESSI-APEC TEL meeting and the e-STG on August 18-19, 2002.

During the discussions, Gyorgy Endersz from the EESSI, provided me with a European Commission Final Report titled "A bridge CA for Europe's Public Administrations, Feasibility Study," which discusses the value of Bridge technology and recommends a prototype be built and pilot implementations by member economies. This report is available at:
<http://europa.eu.int/ISPO/ida/jsps/dsp_showDocument.jsp?printerVersion=1&documentID=581>

The following is a detailed discussion of my participation at the APEC TEL.

Background:

The Asia-Pacific Economic Cooperation (APEC) forum is the primary international organization for promoting open trade and economic cooperation among 21 member 'economies' around the Pacific Rim. The membership is comprised of: Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; Republic of the Philippines; Russia; Singapore; Chinese Taipei; Thailand; USA; and Vietnam. The Telecommunications and Information Working Group (TEL) addresses human resource development; technology transfer and regional cooperation; opportunities for on-site visits, observerships and fellowships; and telecommunications standardization among the APEC member economies.

This year's APEC-TEL was held at the Marriott Renaissance – Moscow, August 17-23. It began with a two day Cybercrime Workshop led by the United States.

EESSI-APEC Meeting

The European Electronic Signature Standard Initiative (EESSI) requested an opportunity to meet with the membership of the APEC TEL e-Security Task Group (e-STG) at TEL 26. Three representatives from EESSI were in attendance. These were: Gyorgy Endersz, Richard Wilsher, and Riccardo Genghini. 13 APEC member economies were also represented.

18-19 August 2002.
Gyorgy Endersz opened the meeting with a brief overview of the EESSI program.

EESSI is a cooperative approach to digital signature. The European Union (EU) Electronic Signature Directive provides a common EU framework for electronic signatures. EESSI was developed to coordinate the implementation of the European Signature Directive. EESSI is industry-led, producing technical standards that the members of the EU are urged to accept. Where possible, this is done through the support of the European Commission. Among its accomplishments is a reference Certificate Policy for Certification Authorities (CA) wishing to issue 'qualified certificates'. Directive Highlights include: Legal recognition of electronic signatures, technology neutrality, and a free flow of products and services. While it excludes any reference or mandate concerning a prior authorization or licensing scheme for Certificate Service Providers (CSP), it does mandate that each EU member must develop a Supervision Scheme for CSPs and calls for the monitoring of a Voluntary Accreditation Scheme in each EU member economy. Four annexes to the Electronic Signature Directive describe various requirements as follows:

Annex 1 – Requirements for qualified certificates
Annex 2 – Requirements for CSPs who issue qualified certificates
Annex 3 – Requirements for secure signature devices
Annex 4 – Requirements for the signature validation process.

The EESSI Steering Group falls under the Information and Communications Standards Board (ICTSB) within the EU, which includes a member of the EU Commission. Under the EESSI Steering Group are two bodies: The European Committee for Standardization/Information Society Standardization System (CEN/ISSS) and the European Telecommunications Standards Institute (ESTI). These two groups work together to provide guidance on implementation of the European Signature Directive. Toward this end, the CEN has developed a common criteria protection scheme for CA signature devices issuing qualified certificates.

This was followed by a description of the APEC structure provided by Steve Orlowski (Australia), Chair of the e-STG as follows:
E-STG decisions must flow back up to the Ministers for adoption. The e-STG has a PKI subgroup dealing specifically with e-Authentication issues. APEC does not make policy/law, however, it does identify best practices, and may make recommendations to standards bodies. APEC does issue cooperative resolutions for standardized performance, however, there is no policy setting.

Discussion ensued in which EESSI revealed it is planning the publication of an "Algo-paper" which will set standards and make recommendations for key lengths, parameters etc. for use in PKI. It was agreed that the APEC member economies would be invited to comment on this document and any others that may ensue.

APEC Perspective – Steve Orlowski

There are three Tiers to electronic signature – Legal, Policy and Technical. APEC has chosen to concentrate on Policy aspects, but finds these are inseparable from legal issues, and that some decisions require technical review.

APEC's goal is universal interoperability between and among APEC members and with other entities with whom interoperability is desirable for APEC members (e.g. EESSI). Four conclusions have been reached concerning APEC and EESSI:

- The two organizations are quite different
- Liaison between the two organizations is necessary
- Liaison must be by member economies not APEC
- Mutual comment/contributions by each to the other's documents is desirable.

EESSI Presentation – Status Information on Trust Service Providers (TSPs) – Richard Wilsher.

Harmonized TSP Status
Goal: Establish a minimum set of common requirements for the provision of harmonized TSP status information and for the means to provide it.
The final technical report has been approved and is available.

Section 3.3 of the EU Directive states: Member States shall ensure establishment of supervisory system for the certification of CA's operating in their economy for the issuance of qualified certificates.

TR 102030 provides the structured requirements

1. Trust Status List (TSL) which contains:
    - information about the scheme
    - information about status issue
    - list of approved TSP's, their approved services, and history of the service's approval status
2. Recognition of X509v3 CRL standard

Next Steps are looming and include establishing a task force to:

Refine some requirements
Develop TSL implementation Standard
Prepare guidance for verification
Conduct some prototyping

Invite multi-national participation/review (next meeting early December)
Task force will begin its work in September 2002 and continue for 12 months.

APEC Response – At TEL 24 the need for transnational recognition of PKI was identified. Differing schemes abound: national roots, bridges, licensing. The goal is that citizens in any APEC economy have access to a certificate that will be accepted by any other APEC economy.

EESSI will make its technical report available to APEC for review by mid-September and include the APEC members in the review list for subsequent drafts. Steve Orlowski will be the APEC liaison for this initiative.

Harmonized Certificate Policies
A fundamental difference between APEC and EESSI is that APEC cannot harmonize. However it can recognize impediments to harmonization and work to remove them. Australia, Singapore and Canada have mapped policies looking for synergies/disconnects. The US is entering the field with intentions to map policies with Canada and Australia. EESSI proposed adding ETSI CA model CP to the mix. The US is mapping the ETSI CP. ETSI will continue exercise with eSTG.

Other considerations
ISO TC68 – Banking Standard CP – extends beyond simple bank use.
Supervisory Schemes (Tscheme (UK), TTML Cooperation (Netherlands))
ISO TC215 – CP standards for Health Care

Harmonization of Accreditation/Licensing Criteria
APEC does not separate licensing/accreditation from CP standardization. The two groups will review their own criteria/standards. Steve Orlowski and Gyorgy Endersz will act as liaisons.

Compendium of IT Security standards and best practice guidelines
Andrew Mason (APEC/NZ) has developed a compendium of Information Systems Security Standards handbook for APEC, however it may be incomplete on National Standards. APEC members and EESSI are invited to comment and provide input. The handbook will be posted for use and revision as necessary. Richard Wiltshire (EESSI) and Andrew Mason (APEC) will handle liaison for this initiative.

Security of the Technical PKI Infrastructures (trustworthy systems, secure devices for signatures/SSCD)
The EESSI strategy is to identify the broadest security guidance for acceptance by ETSI that is Secure, Transparent and Open. This is in accord with the concepts of common criteria and FIPS. There have been recent observations in Europe regarding interactions between the legislative process and technical standardization. The European Signature Directive states that digital signatures are the equivalent of written signatures but each National legislature is applying this unequally. In addition, UNCITRAL provides some relief for organizations operating internationally.

<u>e-STG Meeting, 20 August 2002</u>

1. Report on EESSI meeting

   Gyorgy Endersz provided an overview of the previous day's meeting delineating the following opportunities for collaboration:

   - Individual economies may map policies with ETSI at their discretion

- Information/Requirements for Trusted Service Providers
- Harmonizing (mapping) certificate policies
- Expanded Compendium of Standards
- Assessment Criteria

2. Electronic Authentication Issues Document accepted for publication pending approval by the APEC TEL Ministers.

3. PKI Interoperability Expert Group
A questionnaire concerning legislative/legal underpinnings for electronic signature was conducted among member economies

Key Findings:
- Legislation exists for legal status of e-signature
- Member economies have set technical standards
- There is no consistency in these technical standards

Moving Forward:
- Prepare best practices/broad guidelines for electronic signature
- Continue detailed mapping exercises.

**US offered to participate/assist with both efforts.
APEC agreed to work with the Asia PKI Forum to ensure there is no duplication of effort.

4. Individual Economy Reports
Each economy provided a verbal report based on a submitted written report. Items of note:
- Australian PKI efforts are catalogued at <www.noie.gov.au>
- New Zealand PKI efforts are catalogued at <www.e-government.govt.nz>
- New Zealand has defined four certificate types:
  - Passport certificate
  - Business certificate
  - Associate certificate
  - Anonymous certificate

5. Privacy and Electronic Authentication
ECSG has added privacy to its roadmap
It is developing a plan to map privacy activities in individual economies.
e-STG will ensure its activities are not duplicative and defer to ECSG where necessary.

e-STG Authentication issues ended at this point.

<u>Afterthoughts</u>
Following the meeting, the US Head of Delegation approached me and asked if I would be willing to accept an assignment as the e-STG vice chair. I indicated this would need to be reviewed and accepted by my management.